

Verifying Buchberger’s Algorithm in Reduction Rings

Alexander Maletzky*

Doctoral College “Computational Mathematics” and RISC
Johannes Kepler University Linz, Austria
`alexander.maletzky@dk-compmath.jku.at`

Abstract

In this paper we present the formal, computer-supported verification of a functional implementation of Buchberger’s critical-pair/completion algorithm for computing Gröbner bases in reduction rings. We describe how the algorithm can be implemented and verified within one single software system, which in our case is the Theorema system.

In contrast to existing formal correctness proofs of Buchberger’s algorithm in other systems, e.g. Coq and ACL2, our work is not confined to the classical setting of polynomial rings over fields, but considers the much more general setting of reduction rings; this, naturally, makes the algorithm more complicated and the verification more difficult.

The correctness proof is essentially based on some non-trivial results from the theory of reduction rings, which we formalized and formally proved as well. This formalization already consists of more than 800 interactively proved lemmas and theorems, making the elaboration an extensive example of higher-order theory exploration in Theorema.

Keywords: Buchberger’s algorithm, Gröbner bases, reduction rings, Theorema

1 Introduction

Buchberger’s algorithm was first introduced in [1] for computing Gröbner bases of ideals in polynomial rings over fields. Later, this setting was generalized to so-called *reduction rings* [3, 10], which are essentially unital commutative rings, not necessarily free of zero divisors and not necessarily possessing any polynomial structure. The algorithm the present investigations are concerned with is a variant of Buchberger’s original critical-pair/completion algorithm adapted to the reduction-ring setting. It should not come as a surprise that the increased generality of the underlying domain makes the algorithm slightly more complicated, compared to the case of polynomials over fields. The main differences will be explained in Section 2.

The theory of Gröbner bases, and in particular Buchberger’s algorithm, has already undergone formal treatment of various kinds. For instance, the algorithm was proved correct, e.g., in Coq [11] and ACL2 [9]. A formal analysis of its complexity in some special case was carried out by the author of this paper in [8], and last but not least, the algorithm could even be synthesized automatically from its specification in [6]. However, all of this was done only in the *classical setting*¹, and not in the far more general setting of reduction rings. The *computational* aspect of reduction rings, without formal proofs and verification of any kind, was considered in [4].

*This research was funded by the Austrian Science Fund (FWF): grant no. W1214-N15, project DK1

¹In this paper, the phrase “classical setting” always refers to the case of polynomials over fields.

The software system used both for implementing the algorithm, in a functional-programming style involving pattern-matching and recursion, as well as verifying it, is the Theorema system [5]. Theorema is a mathematical assistant system for all phases of theory exploration: introducing new notions, designing/verifying/executing algorithms, and creating nicely structured documents.

The rest of the document is structured as follows: Section 2 first defines the most important notions and then presents the algorithm in question. Section 3 outlines the main ideas behind the computer-supported formal verification of the algorithm by means of interactive theorem proving in Theorema. Section 4 puts the work described here in a broader context, reporting on the underlying formal treatment of *all* of reduction ring theory in Theorema; readers only interested in Buchberger's algorithm may skip this section. Finally, Section 5 summarizes the content of this paper and hints on possible extensions and future work.

2 The Algorithm

We now outline the algorithm under consideration. For this, let in the remainder of this paper R be a *reduction ring*, i.e. a unital commutative ring, additionally endowed with a partial Noetherian ordering \preceq (among other things, which go beyond the frame of this paper). Before we can state the algorithm, we need to define the concepts of *reduction* and *Gröbner basis*:

Definition 1. Let $C \subseteq R$ and $a, b \in R$. Then a reduces to b modulo C , written $a \rightarrow_C b$, iff $b = a - mc$ for some $c \in C$ and $m \in R$, and in addition $b \prec a$. \rightarrow_C^* and \leftrightarrow_C^* denote the reflexive-transitive and the reflexive-symmetric-transitive closure of \rightarrow_C , respectively.

C is called a Gröbner basis iff \rightarrow_C is confluent.

Algorithm 1 is Buchberger's critical-pair/completion algorithm in reduction rings, given in a functional-programming style with pattern-matching and recursion, and following precisely its implementation in Theorema this paper is concerned with. Sticking to Theorema notation, function application is denoted by square brackets, tuples are denoted by angle brackets, the length of a tuple T is denoted by $|T|$, and the i -th element of T by T_i . Variables suffixed with three dots are so-called *sequence variables* which may be instantiated by sequences of terms of any length (including 0).

As can be seen, function GB only initiates the recursion by calling GBAUX with suitable arguments. GBAUX, in contrast, is the main function, defined recursively according to the three equations (2) (base case), (3) and (4). Please note that termination of GBAUX is by no means obvious, since its second argument, which eventually has to become the empty tuple in order for the function to terminate, may be enlarged by function UPDATE in the second case of (4).

Algorithm 1 Buchberger's algorithm in reduction rings

$$\text{GB}[C] := \text{GBAUX}[C, \text{PAIRS}[|C|], 1, 1, \langle \rangle] \quad (1)$$

$$\text{GBAUX}[C, \langle \rangle, i, j, \langle \rangle] := C \quad (2)$$

$$\text{GBAUX}[C, \langle \langle k, l \rangle, r \dots \rangle, i, j, \langle \rangle] := \text{GBAUX}[C, \langle r \dots \rangle, k, l, \text{CP}[C_k, C_l]] \quad (3)$$

$$\text{GBAUX}[C, P, i, j, \langle \langle b, \bar{b} \rangle, t \dots \rangle] := \quad (4)$$

$$\text{let}_{h=\text{CPD}[b, \bar{b}, i, j, C]} \left\{ \begin{array}{ll} \text{GBAUX}[C, P, i, j, \langle t \dots \rangle] & \Leftarrow h = 0 \\ \text{GBAUX}[\text{APP}[C, h], \text{UPDATE}[P, |C| + 1], i, j, \langle t \dots \rangle] & \Leftarrow h \neq 0 \end{array} \right.$$

The five arguments of function GBAUX have the following meaning:

- The first argument, denoted by C , is the basis constructed so far, i.e. it serves as the accumulator of the tail-recursive algorithm. As such, it is a tuple of elements of R that is initialized by the original input-tuple in equation (1) and returned as the final result in equation (2). Please note that the only place where it is modified is in the second case of (4), where a new element h is added to it (function APP).
- The second argument is a tuple of pairs of indices of the accumulator C . It contains precisely those indices corresponding to pairs of elements of C that still have to be considered; hence, it is initialized by *all* possible pairs of element-indices in (1), using PAIRS, and updated whenever a new element is added to C in (4) using UPDATE.
- The third and fourth arguments, denoted by i and j , are the indices of the pair of elements of C whose critical pairs are currently under investigation.
- The last argument is the tuple containing the critical pairs of C_i and C_j that have not been considered so far. Once initialized by function CP in (3), it is simply traversed from beginning to end without being enlarged by any new pairs.

The most important auxiliary function appearing in Algorithm 1 is function CPD in equation (4). $\text{CPD}[b, \bar{b}, i, j, C]$ returns a ring-element h , which is constructed by first finding g, \bar{g} with $b \rightarrow_C^* g$, $\bar{b} \rightarrow_C^* \bar{g}$ and both g and \bar{g} irreducible modulo C , and then setting $h := g - \bar{g}$. Note that g and \bar{g} are not unique in general, but their concrete choice is irrelevant for the correctness of GBAUX.

Please note that “let” is a Theorema-built-in binder used for abbreviating terms in expressions. In equation (4) $\text{CPD}[b, \bar{b}, i, j, C]$ is abbreviated by h .

Readers familiar with the classical setting might have noticed the following three differences between GBAUX and the classical Buchberger algorithm: Firstly, not only pairs of *distinct* elements C_i, C_j have to be considered, but also pairs of identical constituents; this, in particular, implies that in reduction rings one-element sets are not automatically Gröbner bases. Secondly, one single pair C_i, C_j may give rise to more than one critical pair; this is why CP returns a tuple of critical pairs. Thirdly, in function CPD it is not possible to reduce the difference $b - \bar{b}$ to normal form, even though this would be more efficient.

The algorithm as presented in this paper is not the most efficient one: as in the classical setting there are some improvements that could be applied. For instance, the so-called *chain criterion* [2] could be used to detect “useless” critical pairs, i.e. critical pairs for which h in equality (4) will certainly be 0, without having to apply the (in general computation-intensive) function CPD. Although the chain criterion was introduced only for the case of polynomials over fields, it readily extends to reduction rings, too. Another possible improvement originating from the classical setting consists of immediately auto-reducing each element of the current basis C modulo h in the second case of equality (4); however, it is not yet clear whether employing this improvement will always lead to correct results in the general case of arbitrary reduction rings – this still requires further investigations.

3 The Verification

Function GB has to satisfy four requirements for being totally correct: For a given tuple C of elements of R :

1. the function must terminate,

2. $\text{GB}[C]$ has to be a tuple of elements of R ,
3. the ideal (over R) generated by the elements of $\text{GB}[C]$ has to be the same as the ideal generated by the elements of C , and
4. $\text{GB}[C]$ has to be a Gröbner basis.

The whole verification has been carried out in Theorema, using the proving capabilities of the system. More precisely, each of the four proof obligations, as well as a range of auxiliary lemmata (approx. 160; see Table 1), have been proved *interactively* in a GUI-dialog-based manner: for this, one first needs to initiate a proof attempt by setting up the initial “proof situation”, composed of the formula one wants to prove (“proof goal”) and the list of assumptions one wants to use (“knowledge base”). The system then tries to perform some simple and obvious inference steps (e.g. proving implications by assuming their premises and proving their conclusions), until no more of these simple inferences are possible. Then, the user is asked to decide how to continue, i.e. *which* of the more advanced (and maybe “unsafe”) inferences to apply, *how* to apply them in case there are several possibilities (e.g. providing suitable terms when instantiating a universally quantified assumption), and *where* to continue in the proof search in case the current alternative does not look promising. This process is iterated until a proof is found or the proof search is aborted. Summarizing, it is really the human user who conducts the proof, but under extensive assistance by the system, which in particular ensures that all inference steps are really *correct*. In the remainder of this paper, the term “Theorema-generated proof” always refers to precisely this type of proof.

In the following subsections we address the four proof obligations in more detail.

3.1 Termination

As mentioned already in Section 2, termination is by no means obvious. In fact, if R were not a reduction ring, termination could not even be proved, since one of the axioms characterizing reduction rings is needed only for guaranteeing termination of Algorithm 1. The crucial point is that the second case of (4) can occur only finitely often: this is guaranteed by requiring that in reduction rings there are no infinite sequences of sets D_1, D_2, \dots with $\text{red}[D_i] \subset \text{red}[D_{i+1}]$ for all $i \geq 1$, where $\text{red}[D]$ denotes the set of *reducible elements* modulo the set D . In the second case of (4) it is easy to see that $\text{red}[C] \subset \text{red}[\text{APP}[C, h]]$, meaning that this may happen only finitely many times.

Eventually, termination is proved by finding a Noetherian ordering on the set of all possible argument-quintuples that is shown to decrease in each recursive call of the function. In fact, this ordering is a lexicographic combination of the following two orderings:

1. “ \trianglelefteq_1 ” is defined for subsets of R as $A \trianglelefteq_1 B :\Leftrightarrow \text{red}[B] \subset \text{red}[A]$. This ordering is Noetherian because of the non-existence of certain infinite sequences in reduction rings, as sketched above.
2. “ \trianglelefteq_2 ” is defined for arbitrary tuples as $S \trianglelefteq_2 T :\Leftrightarrow |S| < |T|$. Since the length of a tuple is a natural number, this ordering is clearly Noetherian.

For comparing two argument-quintuples $(C_1, P_1, i_1, j_1, T_1)$ and $(C_2, P_2, i_2, j_2, T_2)$, first C_1 and C_2 are compared w.r.t. \trianglelefteq_1 ; if they are equal, P_1 and P_2 are compared w.r.t. \trianglelefteq_2 ; if they are equal as well, T_1 and T_2 are also compared w.r.t. \trianglelefteq_2 (the indices i and j do not play any role for termination and hence are ignored in the comparison). As one can easily see, the arguments of every recursive call of GBAUX always decrease w.r.t. this lexicographic ordering, which furthermore is Noetherian because its constituents are.

Please note that the formal, Theorema-generated proofs of the remaining three obligations proceed by Noetherian (or “well-founded”) induction on the set of argument-quintuples, based on the Noetherian ordering.

3.2 Type and Ideal

The fact that $\text{GB}[C]$ is a tuple of elements of R is obvious, since the accumulator C is only modified by adding one new ring-element in the recursive call in the second case of (4). Apart from that, it always remains unchanged. Furthermore, even the third requirement can be seen to be fulfilled rather easily: The element h added to C in the second case of (4) is clearly an R -linear combination of elements of C , and hence is contained in the ideal generated by C . This further implies that the ideal does not change when adding h to C .

3.3 Gröbner Basis

The most important requirement is the fourth one. It describes the essential property the output should have, namely being a Gröbner basis – that is why the function is called GB. Gröbner bases play a very important role in computational ideal theory, since many non-trivial ideal-theoretic questions can be answered easily as soon as Gröbner bases for the ideals in question are known. Most importantly, ideal membership and ideal equality can simply be decided by reducing some elements to their unique normal forms modulo the given Gröbner bases.

For proving the fourth requirement we need one of the main results of reduction ring theory, containing a finite criterion for checking whether reduction modulo a given set, or tuple, is confluent. This result was proved formally in Theorema.

Theorem 1 (Main Theorem of Reduction Ring Theory). *Let $C \subseteq R$. Then reduction modulo C is confluent iff for all $c, \bar{c} \in C$ (not necessarily distinct) and all minimal non-trivial common reducibles a of c and \bar{c} there exists a critical pair $\langle b, \bar{b} \rangle$, with $a \rightarrow_{\{c\}} b$ and $a \rightarrow_{\{\bar{c}\}} \bar{b}$, that can be connected below a modulo C .*

The statement of Theorem 1 is somewhat vague. For the precise definition of *minimal non-trivial common reducible* we have to refer the interested reader to [3, 10] or to our recent technical report [7]. Only note that in the classical setting the minimal non-trivial common reducible of two polynomials p and q is precisely the least common multiple of the leading monomials of p and q . Finally, two elements $b, \bar{b} \in R$ are *connectible below* another element a modulo C iff $b \leftrightarrow_C^* \bar{b}$ and every intermediate element in the chain of reductions is strictly smaller than a w.r.t. \preceq .

Now we can outline how function GB can be shown to satisfy the fourth requirement: In (4), if the element h constructed by CPD is 0 then the critical pair $\langle b, \bar{b} \rangle$ can be connected (modulo C) below the minimal non-trivial common reducible a of C_i and C_j it corresponds to; otherwise, b and \bar{b} can certainly be connected below a modulo the enlarged tuple $\text{APP}[C, h]$ (second case). Hence, in either case the critical situation corresponding to $\langle b, \bar{b} \rangle$ is resolved, and the algorithm proceeds with the next critical pair of C_i and C_j , unless all of them have already been dealt with; in that case, the next pair of elements of C is considered (equation (3)). Termination guarantees that at some point *all* pairs of elements of C have been dealt with (even those added in (4)), such that in the end the criterion of Theorem 1 is fulfilled and the output returned by the algorithm is indeed a Gröbner basis.

More formally, the crucial property of GBAUX is the following:

Theorem 2. *For all tuples C of elements in R , all index-pair tuples P , all indices i and j , and all critical-pair tuples M : The result G of $\text{GB AUX}[C, P, i, j, M]$ is again a tuple of elements of R such that all critical pairs of all C_k, C_l , for $\langle k, l \rangle \in P$, can be connected below their corresponding*

minimal non-trivial common reducibles modulo G , and the same is true also for the critical pairs in M .

As mentioned at the end of Section 3.1, the interactively generated Theorema-proof of Theorem 2 proceeds by Noetherian induction on the set of all input-quintuples, distinguishing four cases based on the shape of the input arguments, according to the left-hand-sides of the three equalities (2), (3) and (4) (where the case corresponding to (4) is split into two subcases depending on whether $h = 0$ or not).

The total effort for first formalizing and then verifying Algorithm 1, already knowing Theorem 1, was approximately 70 working hours. As can be seen in Table 1 of the next section, the number of formulas that had to be proved for that purpose is 165.

4 The Formal Treatment of Reduction Ring Theory

What has been presented in the previous sections of this paper actually only constitutes a small fragment of a much larger endeavor: The formalization and formal verification of the theory of reduction rings in Theorema. This project was started two years ago with the aim of representing all aspects of the theory, both theoretic and algorithmic, in a unified and – most importantly – certified way in a computer system. At the moment the whole formalization consists of eight individual components, each being a separate Theorema notebook containing definitions, theorems and algorithms of a particular part of reduction ring theory. Figure 1, which is taken from [7], shows the entire theory graph with all components and their dependencies on each other. The algorithm this paper is concerned with, as well as its correctness proof as described in the previous section, is contained in theory `GroebnerRings`, whereas Theorem 1 together with its proof are contained in theory `ReductionRings`. For more information on the formalization the interested reader is referred to [7]; however, note that there the correctness-proof of Buchberger’s algorithm is still labelled as “future work”, because the proof has been completed only *after* writing the report.

As can be seen from the dashed arrows in Figure 1, the formal verification of some parts of the theory still awaits its completion: the proofs that certain basic domains, namely fields, the integers, integer quotient rings, and polynomials represented as tuples of monomials, are reduction rings have not been carried out yet. This is not because these proofs turned out to be extraordinarily difficult, but rather the opposite: we do not expect any major difficulties there and instead focused on the far more involved proofs (in `ReductionRings`, `Polynomials` and `GroebnerRings`) first, just to be sure that everything works out as it is supposed to. After all, the correctness of Buchberger’s algorithm is absolutely independent of theories `Fields`, `Integers`, etc.

Table 1 lists the sizes of the individual components of the formalization in terms of the numbers of formulas, the numbers of proofs, and the average and maximum proof sizes. Summing things up one arrives at almost 1700 formulas and more than 1100 interactively-generated proofs in the formalization, making it an extensive piece of computerized mathematics.

5 Conclusion

On the preceding pages we described the implementation and formal verification of a non-trivial algorithm of high relevance in computational ideal theory. Although the work is of interest on its own, it also serves as a major case study in how program verification, including the formal development of the underlying theories, can effectively be carried out in the Theorema

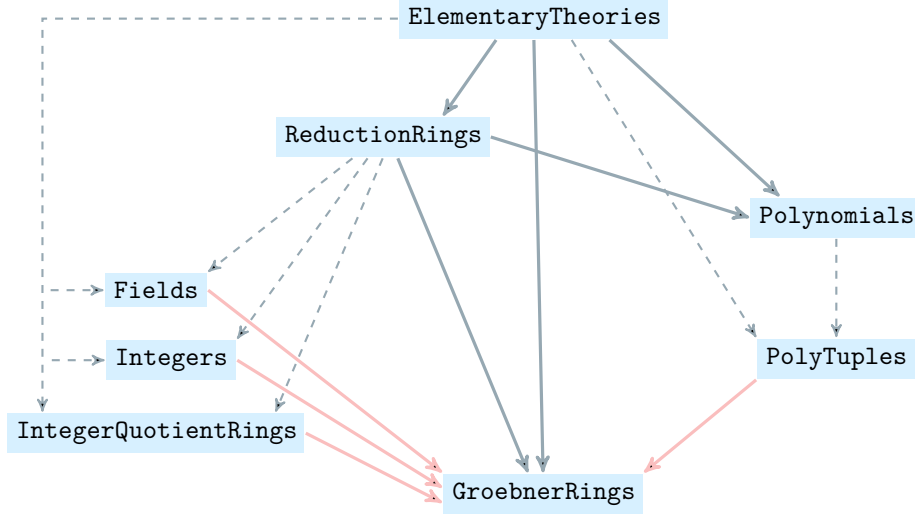


Figure 1: The structure of the formalization. An arrow from A to B denotes dependency of B on A , in the sense that formulas from A are used in B in proofs (gray) or computations (red). Dashed arrows denote future dependencies.

Theory	Formulas	Proofs	Proof Size (avg./max.)
ElementaryTheories	630	390	21.9 / 137
ReductionRings	315	253	38.1 / 198
Polynomials	397	341	45.8 / 322
GroebnerRings	226	165	37.0 / 154
Fields	17	0	
Integers	20	0	
IntegerQuotientRings	19	0	
PolyTuples	66	0	
	1690	1149	34.7 / 322

Table 1: Number of formulas and proofs in the formalization. The proof size refers to the number of inference steps.

system. In addition, most of the elementary mathematical concepts formalized for the present verification, like tuples, (lexicographic) orders and infinite sequences, can be reused for the Theorema-verification of algorithms and programs in completely different areas in the future.

The work described in this paper also revealed a potential improvement of Theorema: Correctness proofs of functional programs are typically achieved following a fixed set of steps, consisting of finding termination orders, proving specialized induction schemas, and using these schemas to prove that certain properties hold for the function, provided they hold for each recursive call. At present, these steps have to be carried out manually, but it is clearly possible to automate the process at least in *some* way – just as in the well-known Isabelle system [12].

Acknowledgements I thank Bruno Buchberger and Wolfgang Windsteiger for many inspiring discussions about Gröbner bases and Theorema, and I also thank the anonymous referees for their valuable comments and suggestions.

This research was funded by the Austrian Science Fund (FWF): grant no. W1214-N15,

project DK1.

References

- [1] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Mathematical Institute, University of Innsbruck, Austria, 1965. English translation in *J. Symbolic Computation* 41(3-4):475–511, 2006.
- [2] Bruno Buchberger. A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Bases. In E. W. Ng, editor, *Proceedings of the EUROSAM 79 Symposium on Symbolic and Algebraic Manipulation, Marseille, June 26-28, 1979*, volume 72 of *Lecture Notes in Computer Science*, pages 3–21. Copyright: Springer, Berlin - Heidelberg - New York, 1979.
- [3] Bruno Buchberger. A Critical-Pair/Completion Algorithm for Finitely Generated Ideals in Rings. In E. Boerger, G. Hasenjaeger, and D. Roedding, editors, *Logic and Machines: Decision Problems and Complexity (Proceedings of the Symposium "Rekursive Kombinatorik", Münster, May 23-28, 1983)*, volume 171 of *Lecture Notes in Computer Science*, pages 137–161, 1984.
- [4] Bruno Buchberger. Gröbner Rings in Theorema: A Case Study in Functors and Categories. Technical Report 2003-49, Johannes Kepler University Linz, SFB F013, November 2003.
- [5] Bruno Buchberger, Wolfgang Windsteiger, et al. *Theorema – A System for Mathematical Theory Exploration*. RISC, Johannes Kepler University Linz. <http://www.risc.jku.at/research/theorema/software/>.
- [6] Adrian Craciun. *Lazy Thinking Algorithm Synthesis in Gröbner Bases Theory*. PhD thesis, JKU Linz, 2008.
- [7] Alexander Maletsky. Exploring Reduction Ring Theory in Theorema. Technical Report 15-11, Research Institute for Symbolic Computation (RISC), Johannes Kepler University Linz, Schloss Hagenberg, 4232 Hagenberg, Austria, 2015.
- [8] Alexander Maletsky and Bruno Buchberger. Complexity Analysis of the Bivariate Buchberger Algorithm in Theorema. In H. Hong and C. Yap, editors, *Mathematical Software – ICMS 2014 (Proceedings of ICMS’2014, August 5-9, Seoul, Korea)*, volume 8592 of *Lecture Notes in Computer Science*, pages 41–48, 2014.
- [9] Inmaculada Medina-Bulo, Francisco Palomo-Lozano, and Jose-Luis Ruiz-Reina. A verified Common Lisp implementation of Buchberger’s algorithm in ACL2. *Journal of Symbolic Computation*, 45(1):96–123, January 2010.
- [10] Sabine Stifter. A Generalization of Reduction Rings. *Journal of Symbolic Computation*, 4(3):351–364, 1988.
- [11] Laurent Thery. A Machine-Checked Implementation of Buchberger’s Algorithm. *Journal of Automated Reasoning*, 26:107–137, 2001.
- [12] Makarius Wenzel et al. *The Isabelle/Isar Reference Manual*, May 2015. <https://isabelle.in.tum.de/>.